Remarks

Preliminarily, it is noted that the Examiner has accepted the changes that applicants have previously made to the specification. It is additionally noted that the Examiner has withdrawn the rejection of applicants' claims 1-10 under 35 U.S.C. § 101.

However, at present, applicants' claims 6-10 stand rejected under 35 U.S.C. § 102(b) based upon the patent to Monier (US patent Number 5,764,554 of record herein). Additionally, claims 1-5 stand rejected under 35 U.S.C. § 103(a) based upon the same patent to Monier. In light of the comments presented below both of these rejections are respectfully but very strenuously traversed. Accordingly, claims 1-10 remain present in the current application.

It is also noted that the present response is being submitted within the two-month period set forth in 37 CFR § 1.136(a). Accordingly, applicants very respectfully request an Advisory Action from the Examiner prior to the three month date of April 11, 2005. In this regard, the Examiner is also invited to provide a telephonic indication of the contents of any Advisory Action at any time prior to that date at the telephone number provided below.

Additionally, as a matter of formality it is indicated that the present responses do not amend applicants' specification or claims in any way. It is also noted that the present response does not require the payment of any additional fees.

Attention is now first directed to the rejection of applicants' claims 1-5 under 35 U.S.C. § 103 based upon the patent to Monier. The untenability of this rejection is clearly demonstrated for all six of applicants' recited claim steps when these steps are considered against the portions of the patent to Monier which the Examiner asserts are corresponding. The table provided below lists each one of applicants' claim steps 1-6 seen in applicants' claim 1. In the rightmost column in the table, there is shown the quotation from the patent to Monier to which the Examiner refers as a basis for supporting the rejection under 35 U.S.C. § 103. None of the cited portions in the Monier patent correspond to steps taken by the applicants. These differences are discussed one by one in the itemized list below.

Step #	**Applicants' Claim 1**	**Monier patent citations**
1	providing a signal representing a constant, *C*, which is equal to 2^{+2mk} mod N	col. 8, line 63: production of $H_1 = 2^{2*n-a}$ mod N' (2*n-1+1 subtractions), for i>1:
2	multiplying said value *A* by said constant *C* using a circuit which accepts two input operands and which produces an output result value Z_0 given by $A\ C\ 2^{-mk}$ modulo *N*	col. 1, line 50: Computation of a parameter H ($H = 2^{m*k}$ mod N) and a parameter J_0 encoded on k bits, with $J_0 = -N_0^{-1}$ mod 2^k, N_0 being the least significant word of the modulo N, and storage of J_0 in a k-bit register 17 col. 7, line 30: II--multiplying the bits of H by C_{i-1}
3	storing said value Z_0 in a first register and in a second register	col. 7, line 64: the s^{th} word of C_i being loaded into the register 16 at any point in time during the above operations
4	for sequential values of an index *i* running from *1* to *t*, repeatedly using the value in said second register as both of said operands for said circuit, with the output of said circuit being stored back into said second register and, when e_{t-i} is *1*, using again the contents of said second register as one input operand to said circuit with said	col. 7, lines 54-62: e) not talking [sic] account of the least significant word of Z(s) and storing the remaining words, namely $Z(s)/2^k$ in the register 11, f) comparing $Z(s)/2^k$ with N', bit by bit, in order to determine the updated value S(s) of the next iteration in the maimer [sic] described here above, this comparison being made by the bit-by-bit subtraction of $Z(s)/2^k$ and N' in the subtraction circuit 29, N' having been delayed by k additional cycles in the delay circuit 33

	other input operand being said Z_0 value in said first register with the output of said circuit being stored in said first register	
5	upon completion of said repetition, operating said circuit with the contents of said second register as one input operand with the constant *1* as said other input operand	col. 7, lines 65-67: R3--at the mth iteration, ignoring the least significant word of Z(m) and entering the remaining words, i.e. $Z(m)/2^k$, into the register 10
6	storing the output of said circuit in at least one of said registers, whereby said at least one register contains the binary representation of A^E modulo *N*	figure 3, element 108: This refers to a block which recites: Add all Ci values to obtain C mod N. Step 108 is discussed in column 6, lines 62-63. col. 6, lines 62-63: E3--performing a modular addition of the C_i values stored and of C_0 or C_0 -N to obtain C mod N (step 108).

Step #1

In applicants' first claim step, there is provided a signal representing a constant which is equal to a particular power of *2* modulo *N* which is typically a large prime number employed in modular arithmetic operations. In contrast, the portion of the Monier patent upon which the Examiner relies teaches the production of a parameter which has a different exponent for the base 2. Furthermore, the modular parameter is *N`* in Monier where $N = N` * 2^a$ (see Monier column 6, lines 4-9). Additionally, the presence of a subscript 1 in the expression H_1 suggests that *H* is a parameter that varies with an index. In contrast, it is seen that applicants' recited constant *C* is indeed a constant which does not depend upon any index value which indicates a particular iteration point. Most relevantly, however, the constant that applicants provide has a different exponent for the base 2. And even if in the Monier patent $n = mk$, the presence of the variable a in Monier's exponent makes it not only different but clearly from all of the above differences obviously quite different. Moreover in this regard, it is to be particularly noted that in applicants' claim the value mk is not equal to n, but is greater than or equal to $n+2$. This step alone is sufficiently different to preclude Monier being employed as a basis for the rejection of applicants' claim 1 under either 35 U.S.C. § 102 or under 35 U.S.C. § 103.

<u>Step #2</u>

In applicants' step 2, there is a multiplication step in which the value A is multiplied by the constant provided in step 1. The value of A referred to in applicants' claim 1 is the base value which is going to be raised to the exponent E. The output of applicants' step 2 is a value Z_0 given by $AC\ 2^{-mk}$ modulo N. In stark contrast, the referenced citation to column 1, line 50 of the patent to Monier upon which the Examiner relies is not even a multiplication step but is instead merely the computation of a parameter. However, the Examiner goes on to cite column 7, line 30 in which a multiplication operation does take place. To the extent that it is the multiplication of a variable by a parameter both the parameter and the variable are different than that which is recited in applicants' second claim step. In particular, it is seen that the parameter H is not the same as the parameter C as employed by the present applicants (see the discussion above with respect to applicants' claim step 1). Furthermore, the multiplication operation referred to in column 7, line 30 is a multiplication not by the total number of bits in the variable C but is rather a multiplication using only a portion of this variable. In this regard, it is noted that C in the patent to Monier refers to one of his input variables. In particular, it is the variable for which he seeks modulo N reduction. In contrast, in applicants' claim 1, the symbol C is used to refer to a constant parameter which is equal to 2^{+2mk} mod M.

Accordingly, it is seen that, even though there is an allusion to a multiplying operation in the cited portion of the Monier patent, the things that are multiplied are significantly different.

Step #3

In applicants' claim step 3, there is a recitation to storing the value Z_0 in a first register and also in a second register. In stark contrast, it is seen that the portion of the patent to Monier upon which the Examiner relies refers to the loading of only a single register. Furthermore, applicants' claim step 3 refers to a step in which the value Z_0 is stored. In stark and utter contrast, the portion of the patent to Monier upon which the Examiner relies refers instead to storing only a portion of the variable *C*. Accordingly, it is seen that not only are the same variable quantities not being stored but Monier incorporates only a storage into a single register. Clearly, the operations recited are not only different but are significantly different.

Step #4

In applicants' claimed step 4 in claim 1, there is a recitation of an iterative process. This iterative process refers to certain bits, e_{t-i} where the values of the variable *e* represent bits in the exponent *E*. In stark contrast, the only similarity between applicants' claim step 4 and the Examiner's citation to column 7, line 54-62, is that there is an iterative process described. However, nowhere in the cited portions of the patent to Monier is there any indication that the cited process or steps include anything whatsoever that could even remotely be construed as an exponent *E*. More will be said about this below.

Furthermore, it is indicated that applicants' claim step 4 refers to a circuit. In particular this circuit is a multiplying circuit. However, in the cited portions of the patent to Monier upon which the Examiner relies (column 7, lines 54-62) there is not one reference whatsoever to a multiplying operation. There is a reference to a possible division operation wherein the divisor is an exponent of the base 2. However, as is well known, such operations are typically carried out as right shift operations. Thus, at the very best the cited portion of Monier refers to a division operation, not to a multiplication operation.

Step #5

Applicants' fifth claim step refers to an operation that occurs upon completion of the iteration step of claim 4. In applicants' recited step, it refers to the operation of the multiplying circuit. This circuit is employed with specific inputs. In short, applicants' claim step 5 is, in effect, a multiplication operation. However in contrast, when one views the cited portion of the patent to Monier upon which the Examiner relies, one is faced not with a multiplication operation but one in which the least significant word of a particular value is ignored with the remaining portion being loaded into a particular register. This is not in any sense the operation of a multiplying circuit modulo *N*.

Step #6

Applicants' claim step 6 refers to the operation of storing the output of the multiplying circuit in one of the registers. Furthermore, applicants' "whereby clause" asserts that the value that is stored in this register is a binary representation of A^E modulo *N*. In short, the output that is stored in one of the registers represents an exponentiation modulo *N*.

Again in stark contrast, the portion of the patent to which the Examiner refers is not directed to modular exponentiation at all but rather to modular reduction. The Examiner refers to a step recited in Monier's Figure 3. This is the final step in his process. In this regard, it is noted that Monier himself describes Figure 3 as a flow chart of "the modular reduction method in one embodiment of the present invention" [emphasis added herein]. Modular reduction is not the same as modular exponentiation. They are significantly different operations. For example, $27 \bmod 5 = 2$ but $27^2 \bmod 5 = 4$. Furthermore, exponentiation is a much more complicated operation. Additionally, while applicants' sixth claimed step refers simply to a storing operation, the cited portion of the patent to Monier refers to an addition operation for the values of C_i. Again, storage is not the same as addition.

It is abundantly clear from the above that applicants' claimed method is not in any way anticipated by nor rendered obvious by the patent to Monier. As previously asserted by applicants' attorney, the patent to Monier is solely directed to modulo reduction operations. In this regard, it is noted that applicants' attorney has downloaded the text of the patent to Monier and has done a search through that text for the words "exponent" or "exponentiation." There are only three places in the text where exponentiation is mentioned. It is mentioned in column 9, line 9, and in column 11, line 50. In both of these instances, the exponentiation refers to an exponent of the number 2. The only other place where the word "exponentiation" is found is in the material following column 17, lines 6-10, where a description of the RSA encryption method is provided. In this regard, it is noted that the patent does not in any way include a description of an exponentiation process, method or operation. The patent teaches only that exponentiation is part of RSA encryption. However, it is clear that the reference indicates that the patent itself is only directed to the advantages of being able to carry out modular reduction operations. That is the sum, substance and limit of the Monier patent. Applicants do not dispute or contend that exponentiation is not part of the RSA encryption algorithm. Applicants do not claim to have invented exponentiation in the modular sense. However, applicants have provided an efficient method for carrying out modular exponentiation in a binary environment.

Furthermore, from the patent text that applicants have downloaded, if there was any reference whatsoever in the patent to Monier for the computation of a value of C to some exponent, one would expect to find within the downloaded text a character string of the form "*C.sup.*". Applicants' search through the downloaded text for this string produced a null result. In particular, applicants' attorney has concluded that if there was any reference at all in the subject patent to producing a value of C^E where E is an exponent, there would be some reference to this string. Its utter absence only confirms applicants' attorney's position that the subject patent is totally devoid of any teachings, disclosure or suggestions for specific methods for carrying out modular exponentiation operations. Accordingly, it is seen that the rejections of applicants' claims 1-5 under 35 U.S.C. § 103 based upon the patent to Monier is untenable. It is therefore respectfully requested that this rejection be withdrawn.

Attention is next directed to the rejection of applicants' claims 6-10 under 35 U.S.C. § 102(b) also based upon the patent to Monier. In this regard, it is noted that a rejection under 35 U.S.C. § 102 is a narrow ground of rejection. It requires each and every recited claim element to be found within the cited patent. Furthermore, these claim elements must be connected in the same way to one another and must also function in the same fashion to produce the same result. Focusing upon this last aspect of the requirement of 35 U.S.C. § 102, it is seen that the structure provided in the patent to Monier does not in any sense whatsoever produce modulo exponentiation results. Monier is solely directed to modulo reduction operations not exponentiation. This should be abundantly clear from the table and discussion provided above.

In a rejection under 35 U.S.C. § 102, it is sufficient to point out a single point of difference. In this regard the Examiner points to Figure 1 in the patent to Monier. This patent characterizes Figure 1 as "a schematic view of a circuit enabling the performance of a modular operation according to the Montgomery Method." However, the patent to Monier characterizes the circuits shown in Figure 1 in a more specific manner beginning in column 1, lines 48-49, wherein it states that the "modular reduction method implemented by the circuit in Figure 1 includes the following stages . . . ." [Emphasis added herein.] Clearly, in the mind of Monier, the circuit shown in Figure 1 is a method for modular reduction. As pointed out above, modular reduction is not the same as modular exponentiation. The only place whatsoever where exponentiation is mentioned in the patent to Monier is in regard to its use in the RSA algorithm. Nowhere is there anything whatsoever taught about a specific method for carrying out modular exponentiation. In particular, the Examiner's attention is directed to applicants' Figure 20 which is described by applicants' claim 6. Nowhere in Monier's Figure 1 is there any teaching, disclosure or suggestion that a particular signal path, register, multiplexor, multiplier, delay or storage circuit accepts, employs, uses, produces or otherwise manipulates a variable that could be described as an exponent such as E in applicants' Figure 20 and as recited in applicants' claim 6. Furthermore, to the extent that Monier describes any kind of a finite state machine, it is clearly and unequivocally not a finite state machine which accepts as an input the value E as shown in applicants' Figure 2 and as recited in applicants' claims. It is abundantly clear that the patent to Monier does not in any sense whatsoever anticipate applicants' claims. Applicants' claims are directed to an apparatus for performing modular exponentiation. Monier only alludes to modular exponentiation but does not describe a process for it. One could allude to a process for separating U^{235} from pitchblende ore but that does not describe a process for it.

The patent to Monier is specifically limited to a process for modular reduction. This is not the same process as modular exponentiation. Accordingly, it is seen that the rejection of applicants' claims 6-10 under 35 U.S.C. § 102(b) is improper. Accordingly, it is respectfully requested that it be withdrawn.

As a final, but very telling matter, it is noted that, in order to support the rejections of applicants' claims, the Examiner was forced to cite portions of Monier that were found in multiple, disparate and disjointed locations which clearly suggest that the Examiner was attempting a hindsight reconstruction of the recited claim steps.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any matters which the Examiner feels could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

MAR. 10, 2005
Date

Lawrence D. Cutter
LAWRENCE D. CUTTER, Sr. Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com